



UNITED STATES PATENT AND TRADEMARK OFFICE

A

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/461,010	12/15/1999	PIERRE CALVEZ	6313	3226

7590 12/14/2005

EDWARD J KONDRACKI
MILES & STOCKBRIDGE PC
1751 PINNACLE DRIVE
SUITE 500
MCLEAN, VA 221023833

EXAMINER

PICH, PONNOREAY

ART UNIT	PAPER NUMBER
----------	--------------

2135

DATE MAILED: 12/14/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

09/461,010

Applicant(s)

CALVEZ ET AL.

Examiner

Ponnoreay Pich

Art Unit

2135

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 15 September 2005.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 20-56 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 20-56 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 9/15/05 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
- Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
- Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|---|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413) |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | Paper No(s)/Mail Date. _____ |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

Claims 20-56 are pending.

Response to Amendment

Applicant's amendments have been noted. Please note new rejections as a result of the amendments below. As a preliminary matter, the examiner notes that the previous office action had 112, second paragraph rejections which applicant did not address in the response filed on 9/15/2005. The errors addressed by these rejections made the meaning and scope of the claims unclear. As they were not addressed, the errors are still present and the meaning and scope of the claims are still unclear. These rejections are repeated below for record along with any new rejections brought about by applicant's amendments. As before, the examiner will attempt to apply art to the best of his understanding of the claims as recited despite the 112, second paragraph errors rendering the meaning of the claims unclear.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claims 20-54 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

1. Independent claims 20, 29, 47, and 51-52 all recite a similar limitation which states "wherein each attribute can at least have the value of pending, in progress, process ended with an error message, process done, sending a

certificate request and done.” The examiner respectfully submits that the some of the values stated above conflict with each other in nature, therefore the use of “and” in the series renders the claims indefinite. For example, something cannot be both “in progress” and “done” at the same time. The examiner believes applicant may have meant to recite, “wherein each attribute can at least have the value of pending, in progress, process ended with an error message, process done, sending a certificate request, or done.” Clarification is requested.

2. Also, for the same limitation recited above for the independent claims, the examiner notes that the limitation seems to be supported in the specification on p9, lines 24-26 and on p10, lines 26-28. However, the specification does not specifically have a limitation wherein the attribute value is “sending a certificate request.” The closest support for this limitation in the specification seems to be “sending a creation request.” The examiner respectfully submits that the limitation of “sending a certificate request” is much broader than “sending a creation request” and in the course of examining this application, the examiner will give the claim language the broadest, reasonable interpretation to “sending a certificate request.”
3. In independent claims 1, 29, and 51, the following limitation is recited: “searching in storage means for one or more attributes.” The examiner respectfully notes that such a limitation was not disclosed in the specification. Instead, on pages 3, 12, 16, and 20 of the specification, searching was instead described as being done for “at least one subject” or “at least one pair of asymmetric keys”. The

examiner respectfully asks applicant to double check the aforementioned independent claims to make sure applicant meant to recite the limitation "searching ... for one or more attributes" instead of what is disclosed in the specification. The examiner suspects that applicant may have meant to recite in the claims that the searching was done for at least one subject or at least one pair of asymmetric keys, which contains one or more attributes.

4. Any claims not specifically addressed are rejected by virtue of dependency.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

Claims 20-21, 29-30, 45-46, 43-56, and 51 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ishii (US 5,768,389) in view of Smith (US 6,651,166) and Andrews et al (US 6,324,645) and further in view of Eigeles (US 6,401,203).

Claim 20:

With regards to Claim 20, the limitation "creating, based on the one or more attributes, at least one first individual creation and certification request for a pair of asymmetric keys for said subject" is met by Ishii on column 11, lines 20-33 and 63-67.

The limitation "transmitting a key generation request corresponding to said first individual creation and certification request to a key generating center (8), which issues

a pair of asymmetric keys in accordance with said key generation request” is met by Ishii on column 11, lines 20-62.

The limitation “creating at least one second individual certification request the public key created for said subject” is met by Ishii on column 11, lines 20-33, 63-67.

The limitation “transmitting a certification authority request corresponding to said second individual certification request to a certification authority, and issuing a first certificate in accordance with said certification authority request” is met by Ishii on column 12 on lines 12-16, 42-46. Further, the limitation of “creating a public key for said subject” is met by Ishii on column 11, lines 60-62. Ishii however does not disclose searching a storage means for the subject that needs the asymmetric keys. This is however disclosed by Smith.

The limitation “searching in storage means for one or more attributes, the attributes specifying one or more subjects for which a pair of asymmetric keys and an associated certificate must be created” is met by Smith et al on column 5, lines 24-35. In Smith, the client information is stored and retrieved (when being compared); afterwards the key pair is generated.

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Smith et al within the system of Ishii because retrieval of the subject’s data from storage is a necessary step towards creation of a pair of keys and a corresponding certificate.

Ishii and Smith do not explicitly disclose the limitation of “wherein each attribute can at least have the value of pending, in progress, process ended with an error message, process done, sending a certification request and done.”

However, Andrews discloses certificates which are associated with encryption keys and users/objects/subjects wherein the status of the certificates is designated and checked (col 1, lines 44-47 and col 6, lines 43-47). This reads on the above-recited limitation. At the time the applicant's invention was made, it would have been obvious to one of ordinary skill in the art to have further modified Ishii and Smith's combination invention using Andrew's teachings. One of ordinary skill would have been motivated to incorporate Andrews's teachings as Andrews teaches that it would allow parties to verify the status of a certificate that is bound to a user as certificates usually expires after a certain amount of time for security purposes (col 5, lines 60-64 and col 6, line 26-30).

Ishii, Smith, and Andrews do not explicitly disclose a subject being a user. However, Eigeles discloses keys and certificates being intended/created for subjects, where the subjects are users and the users having one or more attributes associated with the users (col 3, lines 59-65 and col 4, lines 30-59). It would have been obvious to one of ordinary skill to further modify Ishii's invention such that the keys and certificates were intended/created for users, where the users had attributes associated with them. One of ordinary skill would have been motivated to do so because users are the typical users of digital certificates and keys.

Claim 21:

With respect to Claim 21, the limitation of “creating the pair of keys for a given subject when said subject lacks the pair of keys and the corresponding first individual creation and certification request” is met by Ishii in column 4, lines 16-36; column 28, lines 10-18, 32-38; column 29, lines 30-36, 59-65; column 30, lines 17-20. Subject being a user is obvious to Ishii’s modified invention because it was disclosed by Eigeles as discussed in claim 20.

In light of the above, the limitation recited in claim 21 is obvious to Ishii’s modified invention.

Claim 29:

With respect to Claim 29, the limitation “creating at least one individual certification request for certifying a public key” is met by Ishii on column 11, lines 63-67.

The limitation “transmitting a certification authority request corresponding to said individual certification request to a certification authority, and issuing a certificate in accordance with said certification authority request” is met by Ishii on column 12, lines 12-16 and 42-45; and “creating, based on the one or more attributes, at least one individual certification request for certifying a public key” is met by Ishii on column 11, lines 20-33, 63-67. Ishii however does not disclose searching the storage means for a pair of asymmetric keys. This is disclosed by Smith.

The limitation “searching in storage means for one or more attributes, the attributes associated with one or more subjects for which a certificate must be created” is met by Smith et al on column 5, lines 24-35 and 38-52.

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Smith et al within the system of Ishii because referring back to an already secure storage means for the necessary keys allows the system to save the time it would have used to request and authenticate the sender of the keys from a remote area.

Ishii and Smith do not explicitly disclose the limitation of "wherein each attribute can at least have the value of pending, in progress, process ended with an error message, process done, sending a certification request and done."

However, Andrews discloses certificates which are associated with encryption keys and users/objects/subjects wherein the status of the certificates is designated and checked (col 1, lines 44-47 and col 6, lines 43-47). This reads on the above-recited limitation. At the time the applicant's invention was made, it would have been obvious to one of ordinary skill in the art to further modify Ishii's invention using Andrews teachings. One of ordinary skill would have been motivated to incorporate Andrews's teachings as Andrews teaches that it would allow parties to verify the status of a certificate that is bound to a user as certificates usually expires after a certain amount of time for security purposes (col 5, lines 60-64 and col 6, line 26-30).

Ishii, Smith, and Andrews do not explicitly disclose a subject being a user. However, Eigeles discloses keys and certificates being intended/created for subjects, where the subjects are users and the users having one or more attributes associated with the users (col 3, lines 59-65 and col 4, lines 30-59). It would have been obvious to one of ordinary skill to further modify Ishii's invention such that the keys and certificates

were intended/created for users, where the users had attributes associated with them. One of ordinary skill would have been motivated to do so because users are the typical users of digital certificates and keys.

Claim 30:

With respect to Claim 30, the limitation “certificate for a given subject when said subject lacks the certificate and the individual certification request” is met by Ishii on column 28, lines 10-18, 32-38; column 29, lines 30-36, 59-65; column 30, lines 17-20. Subject being a user is obvious to Ishii’s modified invention because it was disclosed by Eigeles as discussed in claim 29.

In light of the above, the limitation recited in claim 30 is obvious to Ishii’s modified invention.

Claim 45:

With respect to Claim 45, the limitation “comprising performing the encoding of one or more extensions in accordance with one or more given rules and of entering the encoded extension or extensions into the individual certification request during the creation of said individual certification request” is met by Ishii on column 11, lines 63-67 and column 12, lines 1-3.

Claim 46:

With respect to Claim 46, the limitation “changing the value of the attribute contained in each of the individual first and second requests to indicate status of the process” is met by Ishii on Fig. 20 and 21.

Claims 53 and 54:

With respect to Claim 53 and 54, the limitation of “creating a pair of keys for a given subject when a certificate issued in response to a certification authority request for a pair of keys for said subject intended for an identical use has been revoked and a new pair of keys been requested” is met by Ishii on column 28: 10-18, 32-38; column 29, lines 30-36, 59-65; column 30, lines 17-20. Revocation will occur intuitively if the device/key(s) is lost/stolen/destroyed, hence the need to reissue/create a new set of keys. The secret key is reproduced first and the public key is reproduced shortly afterwards. Subject being a user is obvious to Ishii’s modified invention because it was disclosed by Eigeles as discussed in claims 20 and 29.

In light of the above, the limitation recited in claims 53 and 54 is obvious to Ishii’s modified invention.

Claim 55:

Ishii does not disclose, “periodically activating a local registration authority to perform the searching step.” However, this limitation is met by Smith et al on column 5, lines 28-31, 60-62.

Claim 56:

Ishii does not disclose, “wherein an activation period is modifiable.” However, this limitation is met by Smith et al on column 5, lines 28-31, 60-62, so is obvious to Ishii’s modified invention.

Claim 51:

With respect to Claim 51, the limitation “creating, based on the one or more attributes, at least one individual request for creating a symmetric key for said subject”

Art Unit: 2135

is met by Ishii on column 1, lines 26-29, column 11, lines 20-21 and 31-33. A secret key cryptosystem is the same thing as a symmetrical cryptosystem because of the use of the same key to encrypt and decrypt. These symmetrical keys, as disclosed on column 1 are much faster than their asymmetrical counterparts. Hence for the advantage of increasing processing speed, they can intuitively be substituted for the asymmetrical keys in the invention disclosed on column 11.

The limitation "transmitting a key generating request corresponding to said individual creation request to a key generating center" is met by Ishii on column 11, lines 31-33.

The limitation "issuing by said key generating center a symmetric key in accordance with said transmitted key generating request" is met by Ishii on column 11, lines 35-62. Ishii however does not disclose a storage means as disclosed below.

The limitation "searching in storage means for one or more attributes, the attributes specifying one or more subjects for which a symmetric key must be created" is partly met by Smith et al on column 5, lines 24-35. In Smith et al, this input information is retrieved from the SDCE server before the key pair is generated.

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Smith et al within the system of Ishii as to achieve high speed processing.

Ishii and Smith do not explicitly disclose the limitation of "wherein each attribute can at least have the value of pending, in progress, process ended with an error message, process done, sending a certification request and done."

However, Andrews discloses certificates which are associated with encryption keys and users/objects/subjects wherein the status of the certificates is designated and checked (col 1, lines 44-47 and col 6, lines 43-47). This reads on the above-recited limitation. At the time the applicant's invention was made, it would have been obvious to one of ordinary skill in the art to incorporate Andrews teachings with Ishii and Smiths' combination invention because Andrews teaches that it would allow parties to verify the status of a certificate that is bound to a user as certificates usually expires after a certain amount of time for security purposes (col 5, lines 60-64 and col 6, line 26-30).

Ishii, Smith, and Andrews do not explicitly disclose a subject being a user. However, Eigeles discloses keys and certificates being intended/created for subjects, where the subjects are users and the users having one or more attributes associated with the users (col 3, lines 59-65 and col 4, lines 30-59). It would have been obvious to one of ordinary skill to further modify Ishii's invention such that the keys and certificates were intended/created for users, where the users had attributes associated with them. One of ordinary skill would have been motivated to do so because users are the typical users of digital certificates and keys.

Claims 22 and 31-35 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ishii (US 5,768,389) in view of Smith et al (US 6,651,166), Andrews et al (US 6,324,645), and Eigeles (US 6,401,203) in further view of Van Oorschot (US 6,370,249).

Claim 22:

With respect to Claim 22, the combination of Ishii, Smith, Andrews, and Eigeles meets all the limitation except that of periodical generation of keys and certificates.

The limitation "executing said process periodically" is met by Van Oorschot on column 3, lines 14-19. It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Van Oorschot within the combination of Ishii, Smith, Andrews, and Eigeles because a periodical generation of new keys provides a more secure computer system.

Claims 31 and 32:

With respect to Claim 31 and 32, the combination of Ishii, Smith, Andrews, and Eigeles meets all the limitation except that of periodically executing the process.

The limitation "executing said process periodically" is met by Van Oorschot on column 3, lines 14-19. It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Van Oorschot within the combination of Ishii, Smith, Andrews, and Eigeles because a periodical generation of new keys provides a more secure computer system.

Claim 33:

With respect to Claims 33, the limitation "creating the certificate for a given subject when the certificate expires" is met by Ishii on column 12, lines 17-50. Subject being a user is obvious to Ishii's modified invention because it was disclosed by Eigeles as discussed in claim 29.

In light of the above, the limitation recited in claim 33 is obvious to Ishii's modified invention.

Art Unit: 2135

Claims 34 and 35:

With respect to claims 34 and 35 the limitation “creating the new certificate for a given subject when the first certificate expires” is met by Ishii on column 12, lines 17-50. Subject being a user is obvious to Ishii’s modified invention because it was disclosed by Eigeles as discussed in claim 29.

In light of the above, the limitation recited in claims 24 and 35 is obvious to Ishii’s modified invention.

Claims 23-25, 26-28, and 33-43 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ishii (US 5,768,389) in view of Smith et al (US 6,651,166), Andrews et al (US 6,324,645), and Eigeles (US 6,401,203) in view of Van Oorschot (US 6,370,249) and in further view of Aziz (US 6,330,671).

Claims 23-25:

With respect to Claim 23-25, the combination of Ishii, Smith, Andrews, and Eigeles meets all the limitation except that described below.

The limitation “wherein each individual first and second request is created from corresponding multiple creation and certification requests stored in the storage means...” is met by Van Oorschot on column 3, lines 20-38.

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Van Oorschot within the combination

of Ishii, Smith, Andrews, and Eigeles to allow for the secure creation of keys for the required authorized individual.

The combination of Ishii, Smith, Andrews, Eigeles, and Van Oorschot, however, does not disclose a set of subjects belonging to a preset list. This is disclosed by Aziz. The limitation "relative to a set of subjects belonging to a preset list or to a set of subjects defined by predetermined criteria, as well as to model pairs of keys and associated model certificates for the set in question" is met by Aziz on column 4, lines 1-21.

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of further modify Ishii's invention using Aziz's teachings so as to allow for the retrieval of an already authorized list of subjects and hence lessens the likelihood for the creation and transmission of keys to an unauthorized individual. Subject being a user is obvious to Ishii's modified invention because it was disclosed by Eigeles as discussed in claim 20.

In light of the above, the limitation recited in claims 23-25 are obvious to the teachings of Ishii, Smith, Andrews, Eigeles, Van Oorschot, and Aziz.

Claims 26-28:

With respect to Claims 26-28, Ishii does not disclose "searching in each of the multiple creation and certification requests for all of the subjects in a condition such that a pair of keys must be created." However, this limitation is met by Van Oorschot on column 4, lines 37-47.

It would have been obvious to one of ordinary skill in the art at the time the invention was in light of the above to have further modify Ishii's invention according to the incorporate the above recited limitation. One of ordinary skill would have been motivated to do so as to find the correct and authorized recipient of the keys, and hence prevent the sending of keys to an unauthorized individual. Subject being a user is obvious to Ishii's modified invention because it was disclosed by Eigeles as discussed in claim 20.

In light of the above, the limitation recited in claims 26-28 are obvious to the teachings of Ishii, Smith, Andrews, Eigeles, Van Oorschot, and Aziz.

Claims 36-39:

With respect to Claim 36-39, Ishii does not disclose, "creating each individual request from a corresponding multiple certification request recorded in the storage means...." However, this limitation is met by Van Oorschot on column 3, lines 20-38.

It would have been obvious to one of ordinary skill in the art at the time of the invention to incorporate the teachings of Van Oorschot within Ishii's modified invention so as to allow for the secure creation of keys for the required authorized individual.

Ishii also does not disclose the set of keys belonging to a preset list of keys. This is however disclosed by Aziz.

The limitation "...relative to a set of pairs of keys for subjects belonging to a preset list or to a set of pairs of keys for subjects defined by predetermined criteria, as well as to associated model certificates for the set in question" is met by Aziz on column 4, lines 1-21.

It would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate the teachings of Aziz within Ishii's modified invention so as to allow for the retrieval of an already authorized list of subjects and hence lessens the likelihood for the creation and transmission of keys to an unauthorized individual. Subject being a user is obvious to Ishii's modified invention because it was disclosed by Eigeles as discussed in claim 29.

In light of the above, the limitation recited in claims 36-39 are obvious to the teachings of Ishii, Smith, Andrews, Eigeles, Van Oorschot, and Aziz.

Claims 40-43:

Ishii does not disclose "searching in each of the multiple creation and certification requests of the system for all of the subjects in a condition such that a pair of keys must be created." However, this limitation is met by Van Oorschot on column 4, lines 37-47. and subject being a user is obvious to Ishii's modified invention because it was disclosed by Eigeles as discussed in claim 29, so the limitation recited in claims 40-43 is obvious to Ishii's modified invention.

Claim 44 is rejected under 35 U.S.C. 103(a) as being unpatentable over Ishii (US 5,768,389) in view of Smith (US 6,651,166), Andrews et al (US 6,324,645), and Eigeles (US 6,401,203) in further view of Schneier.

With respect to Claim 44, the combination of Ishii, Smith, Andrews, and Eigeles meet all the limitation except for the limitation disclosed below.

Art Unit: 2135

The limitation "wherein each multiple request comprises an attribute relative to at least one execution date and in that said process comprising of including in the search only the multiple requests whose expiration date has arrived" is met by Schneier on page 183-184, section 8.10.

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Schneier within the combination of Ishii, Smith, Andrews, and Eigeles so as to prevent the existence of keys for an extended period of time and hence lessen the likelihood of the keys being compromised as disclosed by Schneier within the above citation.

Claim 47, 48, 52 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ishii (US 5,768,389) in view of Eigeles (US 6,401,203) and further in view of Andrews et al (US 6,324,645).

Claim 47:

With respect to Claim 47 the limitation "a computer system for creating and managing pairs of asymmetrical cryptographic keys and certificates associated with the pairs of keys, the pairs of keys and the certificates being intended for subjects managed by said system, comprising a key generating center for creating at least one pair of keys at the request of a local registration authority with which the key generating center communicates; at least one certification authority to which the

Art Unit: 2135

system has access for creating a certificate at the request of the local registration authority and means for automating, based on one or more attributes associated with one or more subjects, the creation and/or certification of at least one pair of keys for each subject managed by the system” is met by Ishii on column 5, lines 44-67, column 8, lines 8-24 and Fig. 2. In the cited reference, there exists a secret key (private key) generation unit, a public key generation unit and a certification production unit. The tamper resistant personal device represents the local registration authority. It is in communication with the key-generating center. The key-generating center is both the secret/private and public generating center (see Fig. 2). After the user's personal information is entered, the personal device communicates with the other modules within to generate the key pairs and certificate.

Hence, it would have been obvious to have the tamper resistant personal device as the local registration authority because the personal portable device is in communication with the key generating center(s) and requests the creation of a key pair, after the user enters his/her personal information (see Ishii, Fig. 4 and column 7, lines 64-67, column 8, lines 1-3). Furthermore it is obvious that the process of creating and/or certificate of at least one pair of keys is automated because Figure 4 clearly shows that after the user enters his/her personal information, the key pair and certificate is generated without any user intervention. Hence, the process is automated.

Ishii does not explicitly disclose a subject being a user. Ishii does not disclose the limitation of “wherein each attribute can at least have the value of pending, in

Art Unit: 2135

progress, process ended with an error message, process done, sending a certification request and done.”

However, Eigeles discloses keys and certificates being intended/created for subjects, where the subjects are users and the users having one or more attributes associated with the users (col 3, lines 59-65 and col 4, lines 30-59). It would have been obvious to one of ordinary skill to modify Ishii's invention such that the keys and certificates were intended/created for users, where the users had attributes associated with them. One of ordinary skill would have been motivated to do so because users are the typical users of digital certificates and keys.

Further, Andrews discloses certificates which are associated with encryption keys and users/objects/subjects wherein the status of the certificates is designated and checked (col 1, lines 44-47 and col 6, lines 43-47). This reads on the limitation of “wherein each attribute can at least have the value of pending, in progress, process ended with an error message, process done, sending a certification request and done”. At the time the applicant's invention was made, it would have been obvious to one of ordinary skill in the art, in light of Andrews's teachings, to further Ishii's invention according to the limitation recited in claim 47. One of ordinary skill would have been motivated to incorporate Andrews's teachings as Andrews teaches that it would allow parties to verify the status of a certificate that is bound to a user as certificates usually expires after a certain amount of time for security purposes (col 5, lines 60-64 and col 6, line 26-30).

Claim 48:

With respect to Claim 48, the limitation “a central management service for creating, updating and consulting objects and subjects managed by said system a local registration authority for handling the creation and/or the certification of keys intended for the objects and the subjects a central security base containing the subjects and the objects managed by the system with which the local registration authority communicates a key generating center for creating at least one pair of keys at the request of the local registration authority with which the key generating center communicates; and at least one certification authority to which the system has access for creating a certificate at the request of the local registration authority” is met by Ishii on Figure 5.

Ishii does not explicitly disclose subjects being users, i.e. users being managed by the central management service, the keys being intended for the users, and the central security base containing the users.

However, subjects being users is obvious to Ishii's modified invention because it is disclosed by Eigeles as discussed in claim 47.

Claim 52:

With respect to Claim 52, the limitation “a computer system for creating symmetrical cryptographic keys, wherein a symmetrical cryptographic key can be used to both encode and decode data” is met by Ishii on column 1, lines 26-29; and wherein said system manages subjects, characterized in that it comprises a key generating center for creating at least one pair of keys at the request of the local registration authority with which the key generating center communicates; at least one certification

Art Unit: 2135

authority to which the system has access for creating a certificate at the request of the local registration authority and means for automating, based on one or more attributes associated with one or more subjects, the creation of at least one key for each subject managed by the system” is met by Ishii on column 11, lines 50-67 and column 12, lines 1-46.

Ishii does not explicitly disclose a subject being a user. Ishii does not disclose the limitation of “wherein each attribute can at least have the value of pending, in progress, process ended with an error message, process done, sending a certification request and done.”

However, Eigeles discloses keys and certificates being intended/created for subjects, where the subjects are users and the users having one or more attributes associated with the users (col 3, lines 59-65 and col 4, lines 30-59). It would have been obvious to one of ordinary skill to modify Ishii’s invention such that the keys and certificates were intended/created for users, where the users had attributes associated with them. One of ordinary skill would have been motivated to do so because users are the typical users of digital certificates and keys.

Further, Andrews discloses certificates which are associated with encryption keys and users/objects/subjects wherein the status of the certificates is designated and checked (col 1, lines 44-47 and col 6, lines 43-47). This reads on the limitation of “wherein each attribute can at least have the value of pending, in progress, process ended with an error message, process done, sending a certification request and done.” At the time the applicant’s invention was made, it would have been obvious to one of

Art Unit: 2135

ordinary skill in the art, in light of Andrews's teachings, to have further modified Ishii's invention according to the limitation recited in claim 52. One of ordinary skill would have been motivated to incorporate Andrews's teachings as Andrews teaches that it would allow parties to verify the status of a certificate that is bound to a user as certificates usually expires after a certain amount of time for security purposes (col 5, lines 60-64 and col 6, line 26-30).

Claims 49 and 50 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ishii (US 5,768,389) in view of Eigeles (US 6,401,203) and Andrews et al (US 6,324,645) and further in view of Van Oorschot (US 6,370,249).

Claims 49 and 50:

With respect to Claims 49 and 50, all the limitations are met by Ishii, Eigeles, and Andrews except the limitation below.

The limitation of "a wake up mechanism periodically waking up the local registration authority" is met implicitly by Van Oorschot on column 3, lines 14-19. The time-to-time provision of a public key to a client implicitly discloses that the system would need to be alert from at these frequent time intervals and hence this necessitates a wake up mechanism.

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Van Oorschot within the combination system of Ishii and Andrews because a wake up mechanism is necessary for

continuous generation and replacement of old keys and certificates, hence yielding a more current, more secure key generation system.

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Ponnoreay Pich whose telephone number is 571-272-7962. The examiner can normally be reached on 9:00am-4:30pm Mon-Fri.

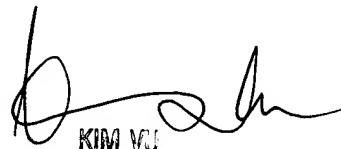
If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 571-272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Art Unit: 2135

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Ponnoreay Pich
Examiner
Art Unit 2135

PP



KIM VU
SUPERVISORY PATENT
TECHNICAL